National Infrastructure Protection Center
CyberNotes

Issue #2001-11 *June 4, 2001*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between May 10 and June 1, 2001. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
ACLogic[1]	Windows 98/98/ME/ NT 4.0/2000	CesarFTP v0.98b	A vulnerability exists due to the plaintext storage of passwords in the 'settings.ini' file, which could let a malicious user gain sensitive information.	No workaround or patch available at time of publishing.	CesarFTP Plaintext Password Storage And Directory Traversal	Medium	Bug discussed in newsgroups and websites. No exploit is required.
ACME Labora-tories[2]	Multiple	Acme.Serve 1.7	A vulnerability exists in the webserver, which could allow a remote malicious user to view sensitive information.	No workaround or patch available at time of publishing.	Acme.Serve Arbitrary File Access	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[1] Bugtraq, May 27, 2001.
[2] Bugtraq, May 31, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Aladdin Knowledge Systems[3]	Multiple	eSafe Gateway 3.0	Vulnerabilities exist in the scripting feature, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	eSafe Gateway Unicode, HTML Tag Script-filtering Bypass	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Aladdin Knowledge Systems[4]	Multiple	eSafe Gateway 2.x	A vulnerability exists in the filtering mechanism, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	eSafe Gateway Script-filtering Bypass	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Apache Group[5]	Windows 98/98/NT 4.0/2000, OS2	Apache 1.3.12win32, 1.3.14win32, 1.3.15win32	A Denial of Service vulnerability exists when an HTTP request consisting of unusual amounts of data is sent to the server.	Upgrade available at: http://httpd.apache.org/dist/httpd/apache_1.3.20.tar.gz	Apache Web Server HTTP Request Denial of Service	Low	Bug discussed in newsgroups and websites.
Beck IPC GmbH[6]	Multiple	IPC@CHIP Embedded-Webserver	Multiple security vulnerabilities exist which could allow a remote malicious user to gain administrative access, reveal sensitive information, and launch a Denial of Service attack.	No workaround or patch available at time of publishing.	IPC@CHIP Multiple Vulnerabilities	Low/**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Cisco Systems[7]	Multiple	IOS 12.1(2)T, 12.1(3)T	A vulnerability exists when a TCP scan is initiated against a piece of Cisco hardware 3100-3999, 5100-5999, 7100-7999, and 10100-10999, which could let a remote malicious user cause an arbitrary reload of the router configuration, and potentially deny service to network assets.	Upgrade available at: http://www.cisco.com	Cisco IOS Router Scan Software Reloading	Low/**High** **(High if DDoS best practices not in place)**	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press and other public media.
Cisco Systems[8]	Multiple	WebNS 4.01B23s, 4.10B13s, 4.0.1, 4.0.1B19s	A vulnerability exists due to insufficient authentication checking, which could let a malicious user gain management privileges without authentication.	Upgrade available at: http://www.cisco.com	Cisco Content Service Switch Management Authentication Bypass	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[3] eDvice Security Services, May 29, 2001.
[4] eDvice Security Services, May 29, 2001.
[5] eSecurityOnline Free Vulnerability Alert 3628, May 14, 2001.
[6] Sentry Research Labs, May 24, 2001.
[7] Cisco Security Advisory, May 24, 2001.
[8] Cisco Security Advisory, CI-01.05.31, May 31, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems[9]	Multiple	CBOS 2.0.1, 2.1.0, 2.1.0a, 2.2.0, 2.2.1, 2.2.1a, 2.3, 2.3.2, 2.3.5, 2.3.7, 2.3.8	Multiple vulnerabilities exist: a vulnerability that permits the successful prediction of TCP Initial Sequence Numbers; a vulnerability that exists when an ECHO REQUEST packet with the record route option is routed through it; a vulnerability caused when passwords, exec and enable, are stored in the cleartext in the NVRAM; and a vulnerability occurring when multiple, large ECHO REPLY packets are routed through an affected Cisco 600 router, causing the router to enter the ROMMON mode and stop passing any further traffic. These vulnerabilities could let a malicious user cause a Denial of Service or gain unauthorized access.	Upgrade available at: http://www.cisco.com.	Multiple CBOS Vulnerabilities	Low/ Medium	Bug discussed in newsgroups and websites. Vulnerabilities have appeared in the Press and other public media.
Computer Associates [10]	Unix	InoculateIT 6.0	A vulnerability exists in ftpdownload, which could let a malicious user create a symbolic link to an arbitrary file that will overwrite the file.	No workaround or patch available at time of publishing.	InoculateIT Symbolic Link File Overwriting	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Computer Associates [11]	Unix	ARCservIT Client version 6.6x	Two tmp-race vulnerabilities exist which could let a malicious user cause a Denial of Service or overwrite existing files.	No workaround or patch available at time of publishing.	ARCservIT Tmp Race Vulnerabilities	Low/ Medium	Bug discussed in newsgroups and websites.
Cosmicperl [12]	Multiple	Directory Pro 2.0	An input validation vulnerability exists in the 'show' variable, which could let a remote malicious user gain sensitive information.	No workaround or patch available at time of publishing.	Directory Pro Arbitrary File Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
DrPhibez and Nitro187[13]	Windows 98/NT 4.0	Guild FTPD 0.9.7	Two vulnerabilities exist: a memory leak in the input parsing code which could cause a Denial of Service; and a buffer overflow in the SITE command which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	GuildFTPD Remote Buffer Overflow and Memory Leak Denial of Service	Low/**High**	Bug discussed in newsgroups and websites.

[9] Cisco Security Advisory, May 22, 2001.
[10] Bugtraq, May 25, 2001.
[11] Bugtraq, May 18, 2001.
[12] Bugtraq, May 27, 2001.
[13] Defcom Labs Advisory, def-2001-27, May 27, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
DrPhibez and Nitro187[14]	Windows 98/NT 4.0	Guild FTPD 0.9.7	Two vulnerabilities exist: user credentials are stored in plain text in a document residing in the program's directory; and a directory traversal vulnerability which could let a remote malicious user gain sensitive information.	No workaround or patch available at time of publishing.	GuildFTPD Plaintext Password Storage and Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
DynFX[15]	Windows NT 4.0/2000	MailServer 2.10 build 3595.1	Buffer overflow vulnerabilities exists in the logon function, which could let a remote malicious user cause a Denial of Service.	Upgrade available at: http://www.dynfx.com/de/downloads/download.asp?app=ms21s.exe	MailServer POP3d Denial of Service	Low	Bug discussed in newsgroups and websites.
Faust Informatics [16]	Multiple	Freestyle Chat 4.1 SR2	Two vulnerabilities exist: a Denial of Service vulnerability exists when a request is submitted to the webserver including the 'AUX' MS-DOS device name; and a directory traversal vulnerability which could let a malicious user gain sensitive information.	Patch available at: http://shop.radiochat.net/redirfaust/downloads/fs_patch_px_p5_urgent.zip	Freestyle Chat MS-DOS Device Name Denial of Service And Directory Traversal	Low/ Medium	Bug discussed in newsgroups and websites. Exploit has been published.
FSU[17]	Unix	DQS (Distributed Queuing System) 3.2.7	A buffer overflow vulnerability exists in the 'dsh' utility program, which could let a malicious user execute arbitrary code/commands with elevated privileges.	Unofficial workaround (Bugtraq): Remove the suid root bit from the program.	DQS 'dsh' Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Gnu[18]	Windows 95/98/ME, Unix	GNU Privacy Guard 1.0-1.0.5	A format string vulnerability exists which can be triggered by attempting to decrypt a file with a specially crafted filename, which could allow a malicious user to gain unauthorized access to the account that attempted the decryption.	Upgrade available at: ftp://ftp.gnupg.org/gcrypt/gnupg/gnupg-1.0.6.tar.gz **Immunix:** http://download.immunix.org/ImmunixOS/ **MandrakeLinux:** ftp://sunsite.ualberta.ca/pub/Mirror/Linux/mandrake/updates/	GnuPG Format String	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Hewlett-Packard[19]	Windows NT 4.0/2000, Unix	OpenView Network Node Manager 6.1	A buffer overflow vulnerability exists due to the unsafe handling of command line input by the Event Correlation Services daemon (ecsd), which could let a malicious user gain elevated privileges and execute arbitrary code.	No workaround or patch available at time of publishing.	OpenView ECSD Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Horde[20]	Multiple	IMP 2.0, 2.2 2.2.1-2.2.4	A vulnerability exists due to insecure use of temporary filenames, which could let a malicious user overwrite files.	Upgrade available at: ftp://ftp.horde.org/pub/imp/tarballs/imp-2.2.5.tar.gz	Imp Message Attachment Symbolic Link	Medium	Bug discussed in newsgroups and websites.

[14] Bugtraq, May 26, 2001.
[15] Strumpf Noir Society Advisories, May 26, 2001.
[16] Bugtraq, May 25, 2001.
[17] Bugtraq, May 19, 2001.
[18] Synnergy Networks, May 29, 2001.
[19] Securiteam, May 29, 2001.
[20] Bugtraq, May 31, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
iPlanet[21]	Multiple	Netscape Enterprise Server 4/SP7	A vulnerability exists when an invalid Method or URI request containing 4022 or more characters is received, which could let a malicious user execute arbitrary code.	Patch available at: http://www.iplanet.com/products/iplanet_web_enterprise/iwsalert5.11.html	Netscape Enterprise Server Method and URI Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[22]	Windows 2000	Windows 2000, 2000 SP1	A vulnerability exists in the handling of debug registers, which could let a malicious user elevate their privileges to have write access to C:\WINNT\SYSTEM32 and HKCR (The registry root key HKEY Classes Root).	Microsoft SP2 fixes this issue available at: http://download.microsoft.com/download/win2000platform/SP/SP2/NT5/EN-US/W2KSP2.exe	Windows 2000 Debug Registers	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[23] ***Net Exploit released***[24]	**Windows 95/98/98 SE/98 ME/NT 4.0**		**A remote Denial of Service vulnerability exists in NetBIOS.** **Note: This vulnerability affects many operating systems aside from Microsoft Windows; however, Microsoft is the only vendor so far that has issued a patch and workaround.**	**Microsoft has released a patch for Windows NT 4.0. For those running Windows 95/98/ME, Microsoft recommends disabling File and Printer Sharing. Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-091.asp**	**Windows Incomplete TCP/IP Packet** **CVE name CAN-2000-1039**	**Low**	**Bug discussed in newsgroups and websites.** ***Exploit script has been published.***
Microsoft[25]	Windows 95/98/NT 4.0/2000	Windows Media Player 6.4, 7	Two vulnerabilities exist: a vulnerability in the implementation of Windows Media Player which could disclose sensitive information; and a buffer overflow vulnerability created by the way ASX files are handled (associated video/x-ms-asf MIME type), which could let a remote malicious user execute arbitrary code. A privacy issue also exists which could enable a malicious set of web sites to uniquely identify visitors through profiling.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-029.asp	Windows Media Player Internet Shortcut Execution And Buffer Overflow CVE Name: CAN-2001-0242, CAN-2001-0243	**High**	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerabilities have appeared in the Press and other public media.
Microsoft[26]	Windows 95/98/NT 4.0/2000	Word 2000 SR1	A vulnerability exists due to .asd files not being checked for macros, which could allow macros to execute without the user's knowledge.	Word Mail Merge Security Update available at: http://support.microsoft.com/support/kb/articles/Q274/2/28.asp	Microsoft Word .asd Macro File Execution	Medium/ **High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[21] Securiteam, May 24, 2001.
[22] Georgi Guninski Security Advisory #45, May 24, 2001.
[23] Microsoft Security Bulletin, MS00-091, November 30, 2000.
[24] Securiteam, May 24, 2001.
[25] Microsoft Security Bulletin, MS01-029, May 23, 2001.
[26] SecurityFocus, May 23, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[27]	Windows 95/98/NT 4.0/2000, MacOS	Word 97 SR1, SR2, 98, 98 for Mac, 2000 SR1, SR1a, SR2, 2001 for Mac	A vulnerability exists in Word, which does not properly check for macros in RTF template documents. This vulnerability could enable a malicious user to create a document that, when opened in Word, would run a macro without asking for the user's permission.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-028.asp	Microsoft Word RTF Template Macro Execution CVE Name: CAN-2001-0240	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the Press and other public media.
Microsoft[28] ***Microsoft re-releases bulletin***[29]	**Windows 98/9se/ME/ NT 4.0/2000**	**Windows 98, 98SE, ME, 2000 (Hilgraeve Hyper Terminal 6.0 and previous)**	**A security vulnerability exists in the HyperTerminal application that ships with several Microsoft operating systems which could allow a malicious user to execute arbitrary code.** ***Microsoft re-released the bulletin to advise of the availability of a new patch that corrects both this vulnerability and a subsequently discovered variant.***	**Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-079.asp**	**Hyper Terminal Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites. Exploit has been published.** ***Vulnerability has appeared in the Press and other public media.***
Microsoft[30] ***Microsoft updates bulletin.***[31] ***Microsoft re-releases bulletin***[32]	**Windows NT/2000**	**Microsoft SQL Server 7.0** ***Enterprise Manager Server***	**The Data Transformation Service (DTS) component of SQL 7.0 allows a malicious user the ability to compromise database passwords.** ***Microsoft updated this bulletin to reflect a similar issue with the Enterprise Manager Server registration dialog.*** ***Bulletin was later revised to reflect a patch available for SQL Server 7.0 Service Pack 3 and a password removal tool.***	**Patch available at:** **Intel:** **http://www.microsoft.com/Downloads/Release.asp?ReleaseID=21905** **Alpha:** **http://www.microsoft.com/Downloads/Release.asp?ReleaseID=21906** ***A new version of the patch is available to remedy all symptoms related to this vulnerability.*** ***A patch is available to fix this vulnerability. Please read the Security Bulletin at:*** http://www.microsoft.com/technet/security/bulletin/ms00-035.asp	**SQL Server DTS Password**	**Medium**	**Bug discussed in newsgroups and websites. Exploit has been published.**
MIMAnet[33]	Multiple	Source Viewer 2.0	A directory traversal vulnerability exists which could let a remote malicious user view sensitive information.	No workaround or patch available at time of publishing.	Viewer Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[27] Microsoft Security Bulletin, MS01-028, May 21, 2001.
[28] Microsoft Security Bulletin, MS00-079, October 18, 2000.
[29] Microsoft Security Bulletin, MS00-079 (version 2.0), May 25, 2001.
[30] Microsoft Security Bulletin, MS00-035, June 15, 2000.
[31] Microsoft Security Bulletin, MS00-041, July 12, 2000.
[32] Microsoft Security , Bulletin MS00-035 (version 2.0), May 10, 2001.
[33] Bugtraq, May 23, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
NetBSD[34]	Unix	NetBSD 1.4, 1.5, -current	A Denial of Service vulnerability exists when multiple bogus fragmented IPv4 packets are transmitted.	Information about upgrade can be found at: ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2001-006.txt.asc	NetBSD Bogus Fragmented IPv4 Packet Denial of Service	Low	Bug discussed in newsgroups and websites.
NetBSD[35]	Unix	NetBSD 1.4.1 sh3, 1.5 sh3	A vulnerability exists in the ports of NetBSD for the Hitachi SuperH architecture in their implementation of sigreturn(), which could let a malicious user gain supervisor privileges and compromise root.	Patch available at: ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2001-008.txt.asc	NetBSD Super-H Port sigreturn() Input Validation	**High**	Bug discussed in newsgroups and websites.
NetBSD[36]	Unix	NetBSD 1.4, 1.5, -current	A vulnerability exists in IP Filter (ipf) due to incomplete checks on a fragmented packet, which could let a malicious user bypass filter rules.	Patch available at: ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2001-007.txt.asc	NetBSD IP Filter Bypass	Medium	Bug discussed in newsgroups and websites.
Omnicron Technologies Corporation[37]	Windows 98/98/NT 4.0/2000	Omni HTTPD 2.0.4-2.0.8	Two vulnerabilities exist: a Denial of Service vulnerability exists when numerous requests for PHP scripts are submitted; and a vulnerability created by submitting a specially crafted GET request for a known file (.php, .pl, or .shtml), which could let a malicious user gain sensitive information.	No workaround or patch available at time of publishing.	OmniHTTPD PHP Denial of Service And File Source Disclosure	Low/ Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Oracle[38] ***Patch available[39]***	**Windows 98se/NT 4.0/2000**	**Application Desktop Integrator 7.1.1.10.1**	**A vulnerability exists in the default configuration for plain text password storage, which could let a malicious user gain access to the APPS Schema password and potentially full access to the database.**	***Patch available at: http://metalink.oracle.com***	**Oracle ADI Plain Text Password Storage**	**Medium**	**Bug discussed in newsgroups and websites. Exploit has been published.**
Pi-Soft[40]	Windows 95/98/ME/ NT 4.0/2000	SpoonFTP 1.0, 1.00.12	Buffer overflow vulnerabilities exists in the 'CWD' and 'LIST' commands, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.pi-soft.com/spoonftp/index.shtml	SpoonFTP 'CWD' and 'LIST' Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Qualcomm[41]	Windows 95/98/NT 4.0/2000	Eudora 5.1	A vulnerability exists which could let a malicious user execute arbitrary code if the 'Use Microsoft viewer' option is enabled.	Unofficial workaround (Bugtraq): Disable the 'Use Microsoft Viewer' option.	Eudora Hidden Attachment Execution	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[34] NetBSD Security Advisory, 2001-006, May 30, 2001.
[35] NetBSD Security Advisory, 2001-008, May 30, 2001.
[36] NetBSD Security Advisory, 2001-007, May 30, 2001.
[37] Securiteam, May 29, 2001.
[38] Securiteam, May 8, 2001.
[39] Securiteam, May 27, 2001.
[40] Strumpf Noir Society Advisories, May 30, 2001.
[41] Bugtraq, May 28, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SCO[42]	Unix	Open Server 5.0, 5.0.1-5.0.6, UnixWare 5.x	A vulnerability exists in the vi editor which creates temporary files in /tmp without checking if the file already exists. This could let a malicious user overwrite existing files.	No workaround or patch available at time of publishing.	vi Insecure Temporary File Creation	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Sendmail Consortium[43]	Multiple	Sendmail 8.10-8.12Beta 7	Several race condition vulnerabilities exist, which could let a malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.sendmail.org/pub/sendmail/sendmail.8.11.4.tar.gz	Sendmail Unsafe Signal Handling Race Condition	High	Bug discussed in newsgroups and websites.
Spearhead Security[44]	Multiple	NetGAP 200, 300	A vulnerability exists which could let a remote malicious user bypass the filtering function and gain access to restricted resources.	No workaround or patch available at time of publishing.	NetGAP Escaped And Encoded URL Filtering Bypass	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Spytech[45]	Windows 95/98/ME/ NT 4.0/2000	Spy Anywhere 1.50	A vulnerability exists when a single character is placed in the 'loginpass' field when supplying authentication credentials, which could let a malicious user gain administrator privileges.	The vendor has acknowledged the issue, which will be addressed in SpyAnywhere version 2.0 to be released this summer.	SpyAnywhere Unauthorized Administrator Access	High	Bug discussed in newsgroups and websites. Exploit has been published.
Sun Micro-systems, Inc.[46]	Unix	Solaris 8.0	A buffer overflow vulnerability exists in the mailtool program included with OpenWindows, which could let a malicious user execute arbitrary code/commands.	No workaround or patch available at time of publishing.	Solaris mailtool Buffer Overflow	High	Bug discussed in newsgroups and websites.
Symantec[47]	Windows 95/98/NT 4.0/2000	Norton AntiVirus 2000.0	A buffer overflow vulnerability exists in poproxy.exe, which could let a malicious user execute arbitrary code.	Patch available by running LiveUpdate. Information on how to run LiveUpdate available at: http://service1.symantec.com/SUPPORT/sharedtech.nsf/docid/1999121613163206&src=w	Norton Anti-Virus 2000 POProxy.exe Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit has been published.
Texas Imperial Software[48]	Windows 95/98/NT 4.0/2000	WFTPD 3.0, 3.00R3-3.00 R5, 3.00R4-3.00 R5 Pro	A buffer overflow vulnerability exists when a user requests a 'LIST' of the current directory or 'LIST -d' of a directory that could allow a remote malicious user to execute arbitrary code, and a directory traversal vulnerability exists that could let a malicious user gain sensitive information.	No workaround or patch available at time of publishing.	WFTPD Path/File Mapping Buffer Overflow And Directory Traversal	High	Bug discussed in newsgroups and websites. No exploit is required for the buffer overflow vulnerability. Exploit has been published for the directory traversal vulnerability.

[42] Strategic Reconnaissance Team Security Advisory, SRT2001-9, May 22, 2001.
[43] RAZOR Advisory, BV-015, May 28, 2001.
[44] Securiteam, May 28, 2001.
[45] Strumpf Noir Society Advisories, May 23, 2001.
[46] Bugtraq, May 28, 2001.
[47] Bugtraq, May 24, 2001.
[48] Bugtraq, May 24, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Trend Micro[49]	Windows NT 3.5/3.51/ 4.0	InterScan VirusWall for Windows NT 3.4, 3.5, 3.51	A vulnerability exists in the management interface, which could let a remote malicious user make modifications for the configuration of software.	No workaround or patch available at time of publishing.	InterScan VirusWall Remote Reconfigura-tion	Medium	Bug discussed in newsgroups and websites. Exploits have been published.
TWIG[50]	Multiple	TWIG 2.0- 2.6.1	A vulnerability exists because the application fails to quote form variables when they are included in SQL query strings, which could let a malicious user perform unauthorized operations.	No workaround or patch available at time of publishing.	TWIG Webmail SQL Query Modification	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Webmin[51]	Unix	Webmin all versions prior to 0.85	A vulnerability exists because sensitive information stored in certain environment variables is not properly deleted, which could let a malicious user gain root privileges.	Upgrade available at: http://www.webmin.com/webmin/	Webmin Environment Variable Information Disclosure	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
XChat[52]	Unix	X-Chat version 1.2.x	A format string vulnerability exists which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	X-Chat Format String	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine, and the machine responds with a command prompt with administrator privileges.

Medium - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such a vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of a medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between May 21 and May 31, 2001, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 18 scripts,

[49] SNS Advisory No.28, June 1, 2001.
[50] Bugtraq, May 28, 2001.
[51] Bugtraq, May 26, 2001.
[52] Securiteam, May 29, 2001.

programs, and net-news messages containing holes or exploits were identified. *At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script Name	Script Description
May 31, 2001	Gnupig.tar.gz	Exploit for the Gnupg v1.0.5 format string vulnerability.
May 30, 2001	Lcrzosrc-3.12.tgz	A toolbox for network administrators and network hackers that contains over 200 functionalities to sniff, spoof, create clients/servers, create decode and display packets, etc.
May 30, 2001	**Omnised.pl**	**Perl script which exploits the OmniHTTPD v2.08 for Windows 98/ME/NT/2000 vulnerability and allows you to dump the source of php Perl and other files to a text file.**
May 30, 2001	**Requiem.c**	**Script which exploits the HP OpenView ECSD Buffer Overflow vulnerability.**
May 29, 2001	**Script38a.zip**	**Script which exploits the eSafe Gateway Unicode, HTML Tag Script-filtering Bypass vulnerabilities.**
May 28, 2001	**HeyDORA.txt**	**Technique for exploiting the Qualcomm Eudora Hidden Attachment Execution vulnerability.**
May 27, 2001	JMScan	A Java based scanning tool, which scans remote hosts for vulnerabilities.
May 25, 2001	Adore-0.38.tar.gz	A Linux LKM based rootkit for Linux v2.[24] which features smart PROMISC flag hiding, persistent file and directory hiding (still hidden after reboot), process-hiding, netstat hiding, rootshell-backdoor, and an uninstall routine.
May 25, 2001	**Xchat.c**	**Exploit script for the X-Chat v1.2.x format string bug vulnerability.**
May 24, 2001	**crackipc-0.2b.zip**	**Script which exploits the IPC@CHIP Multiple Vulnerabilities.**
May 24, 2001	pipe3.cpp	Script which exploits the MS Windows 2000 Debug Registers vulnerability.
May 23, 2001	Linkmax.txt	The WebAvail LinkMax2 (ASP) allows website visitors to view the LinkMax2 admin login and password.
May 23, 2001	Modhide1.c	Program which demonstrates a new method of hiding kernel modules that does not trigger any normal detection techniques because it does not change lsmod or the system call table. Instead it hacks the kernel's memory to make it "forget" the module.
May 23, 2001	Original.doc	Exploit technique for the Microsoft Word .asd Macro File Execution vulnerability.
May 21, 2001	**Dqsexp.c**	**Script which exploits the DQS dsh Buffer Overflow vulnerability.**
May 21, 2001	Dscan-0.1.1src.tar.gz	A distributed port scanner that scans from many hosts, making it harder to detect.
May 21, 2001	Isnprint.c	Program which displays the ISN numbers of a remote server.
May 21, 2001	Nbtstream.c	A NetBIOS session request flooder which exploits the vulnerability discussed in MS00-091.

Trends

Probes/Scans:

CERT/CC continues to observe increased network reconnaissance activity and a significant increase in the number of generalized port scans of hosts.

The CERT/CC has observed in public and private reports a recent pattern of activity surrounding probes to TCP port 10008. An artifact called the 'cheese worm' may contribute to the pattern. For more information, please see CERT® Incident Note IN-2001-05, located at: http://www.cert.org/incident_notes/IN-2001-05.html

There has been an increase in the number of scans and attacks to port 515 looking for the LPRng User-Supplied Format String vulnerability, Wu-Ftpd Remote Format String Stack Overwrite Vulnerability, the ISC Bind 8 Transaction Signatures Buffer Overflow Vulnerability, and the rpc.statd Remote Format String Vulnerability.

Other:

The CERT/CC has received several inquiries about an e-mail virus warning currently in circulation on the Internet. The e-mail contains several language translations of a virus warning related to the file SULFNBK.EXE. This e-mail message is a HOAX. Although the SULFNBK.EXE file may be infected by a number of valid viruses, the mere presence of the file as described in the message is not a sign of a virus infection. The SULFNBK.EXE file is a legitimate Microsoft Windows utility that is used to restore long file names.

Recent reports on IIS vulnerabilities and the large amount of NT servers being penetrated using different exploits have raised the need to tighten the security of IIS version 5.0 servers. Please see the IIS version 5.0 checklist at: http://www.microsoft.com/technet/security/iis5chk.asp.

CERT/CC has received reports of a new piece of self-propagating malicious code referred to as the sadmind/IIS worm. The worm uses two well-known vulnerabilities to compromise systems and deface web pages: A two-year-old buffer overflow vulnerability in the Solstice sadmind program; and, after successfully compromising the Solaris systems, a seven-month-old vulnerability which compromises the IIS systems. For more information, please see CERT® Advisory CA-2001-11, located at: http://www.cert.org/advisories/CA-2001-11.html.

There has been a very significant increase in attempts to exploit known weaknesses in the lpd/LPRng and RPC daemons (ports 515 and 111) of Unix-based operating systems. For more information, please see NIPC ALERT 01-010, located at: http://www.nipc.gov/warnings/alerts/2001/01-010.htm.

The NIPC has issued an advisory concerning an unchecked buffer vulnerability in an Internet Service Application Program Interface (ISAPI) extension that could allow the compromise of an IIS 5.0 web server. For more information, please see NIPC ADVISORY 01-011, located at: http://www.nipc.gov/warnings/advisories/2001/01-011.htm.

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

IRC.Cuty (Alias: Elspy.a.worm) (IRC Worm): This worm is an encrypted DOS executable file. When it is executed, it decrypts itself, creates the Cutyjant.bat file in the same folder as the worm, and executes it. The batch file copies the last .doc file from the folder that contains Cutyjant.bat to C:\Mirc\Cutyjany.doc. It also creates a Script.ini file in the C:\Mirc folder. (NOTE: If the C:\Mirc folder does not exist, the worm drops the Script.ini in the folder that contains Cutyjant.bat.) If no .doc files exist in that folder, the C:\Mirc\Cutyjany.doc file not created. The worm uses the mIRC Internet Relay Chat software to distribute C:\Mirc\Cutyjany.doc file to IRC users. This worm contains some faulty code.

Linux/Cheese (Aliases: Cheese, Linux.Cheese.Worm) (Linux Worm): This worm will only affect Linux systems previously infected with the Linux/Lion worm. When a machine is infected by the worm, it will extract the worm to the /tmp/.cheese directory and then blank any lines in /etc/inetd.conf which contain the text '/bin/sh'. (A line containing this text is added as a backdoor when a computer is infected with Linux/Lion.) The worm will then scan for other computers with the backdoor left open by Linux/Lion.

HTML_BOMB.A (Alias: BOMB.A) (HTML Virus): This malicious HypterText Mark-up Language (HTML) file opens an infinite number of browser windows until it has consumed all of the memory resources, causing the system to hang. The process of this program can be stopped when this malicious program is terminated or closed.

PE_MADONNA.A (Aliases: MADONNA, MADONNA.A) (File Infector Virus): This Win32 direct-infector virus overwrites infected Portable Executable (PE) files in the Windows directory and then attempts to send e-mails. Upon execution, it modifies the title bar. When the system time is equal to 11:00 p.m., it displays a message and shuts down

the computer. When the current system date is Friday the 13th, it displays a message, formats the infected system's drive C:\, and then restarts the computer.

VBS.Devolve.A (Visual Basic Script Worm): If the infected HTML file is opened, the virus uses the object function in Microsoft Word to search drive C for HTML files to infect. On the 15th or 30th of every month, the virus modifies the Autoexec.bat file to repeatedly display the following message:

this computer waz infected from dr[kazoy]
A Demo Html Virus called tvkid
Hello Tvkid
Press any key continue . . .

If you press any key, the message "Hello Tvkid" is displayed. To avoid this, Press Ctrl+C to cancel.

VBS/Lovelet-CM (Aliases: Jennifer Lopez, VBS.Loveletter.CM@mm) (Visual Basic Script Worm):
This is an e-mail-aware worm. The worm copies itself to a file called JENNIFERLOPEZ_NAKED.JPG.vbs in the Windows directory. It then forwards itself via e-mail to every contact in the Microsoft Outlook address book with the following characteristics:

Subject: Where are you?
Body text: This is my pic in the beach!
Attached file: JENNIFERLOPEZ_NAKED.JPG.vbs

When the attached file is opened, the worm searches all fixed and network drives for files with extensions .VBS, .VBE, .JS, .JSE, .CSS, .WSH, .SCT, .HTA, JPG, .JPEG, .MP2 and .MP3. The worm overwrites all found files. Original extensions .JS, .JSE, .CSS, .WSH, .SCT and HTA are changed to .VBS. Original extensions .JPG and. JPEG are converted to double extension. JPG.VBS and. JPEG.VBS respectively. Attributes of the original files with .MP2 and .MP3 extension are changed so that the original file is hidden and the worm creates a new file with the identical name and VBS extension. The worm also creates the Registry keys HKCU\software\ JENNIFERLOPEZ_NAKED\ so that it contains the text "Worm made in algeria" and HKLM \SOFTWARE\Microsoft\ Windows\CurrentVersion \Run, so that it contains the name of the worm file. The worm then sends itself to all contacts found in the Microsoft Outlook address book. Finally it drops and runs a file infected with a variant of the highly destructive W95/CIH virus (also known as Chernobyl). The dropped file is detected by SAV as W95/CIH-10xx.

VBS_NFLIGHT.A (Alias: NFLIGHT.A) (Visual Basic S cript Worm): This Visual Basic Script (VBS) worm propagates via e-mail in Microsoft Outlook. It requires the WSCRIPT/CSCRIPT to execute properly. It does not have a destructive payload. The worm also disables various security features in an infected system such as:

Setting the security level of Internet Explorer to low
Setting the security level in WSH to low
Allowing remote scripting in WSH
Disabling MS Outlook's warning message when a VBS file is opened
The worm has other capabilities that include:
When the current system day is the 5th of any month, it disables the desktop
Change the registered name to "NightFlight" and the registered organization to "Carpe Noctem"
Change the wallpaper to a random bitmap found in the Windows folder.
Add the entry "Start with NightFlight" when the user right-clicks any file or folder. When this entry is selected the worm executes.

Thereafter, it sends e-mails to all addresses in the contact list. Instead of embedding the worm to the mail, it attaches the worm to the e-mail message body. This worm's source code will not execute. It also searches for network drives mounted in the infected system that grant write access so that it can copy its viral file HELP.TXT.VBS. It modifies the file SCRIPT.INI so that it sends copies of itself to all users connected in the mIRC channel that the infected user logs on to. If a Microsoft Agent is installed in the system (this is installed by default in Windows 98 SE), it executes the agent and then displays the character of Merlin and the following text string: "The NightFlight is still out there!"

VBS.NoMercy.A (Aliases: VBS/NoMercy.a, VBS.NMVT) (Visual Basic Script Worm): If an infected file is executed, the virus searches for .html, .htm, .shtml, .stm, and .asp files in the same folder as the virus.
If the virus finds files to infect, it inserts its code at the beginning of the file. On the 13th or 30th of every month, the virus displays the message: "God, why you did it to me."

VBS_NOPED.A (Alias: NOPED.A) (Visual Basic Script Worm): This encrypted mass-mailing worm is written in Visual Basic Script (VBS). It propagates via Microsoft Outlook or Outlook Express, and arrives as an e-mail attachment "END ILLEGAL child porn NOW.TXT.vbs." It modifies registry entries, but carries no destructive payload. Upon execution, and when the current system date is May 1, 2001 or later, this virus modifies the property of the e-mail it sends to the following or to garbage characters:

Subject: FWD: Help us ALL to END ILLEGAL child porn NOW

Message Body: Hi, just a quick e-mail. Please read the attached document as soon as you can.
Thanks.

It then modifies the registry to change the homepage of Internet Explorer:

HKCU\Software\Microsoft\Internet Explorer\Main\Start Page
http://www.geocities.com/antipedo2001
HKCU\Software\Microsoft\Internet Explorer\Main\Window Title
"|.,.-*^*-.,.\ FUAHACKEDU@888.NU /.,.-*^*-.,.|"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Fua "wscript.exe (infected file) %"
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\1 (infected file), "REG_SZ"
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\2(infected file), "REG_SZ"

If the registry entry in the following is not equal to zero (0), it executes its mass-mailing routine. If the value in the following registry entry is less than the number 6, it subtracts the value from the number of entries in the infected user's Address Book. The number of e-mails it sends depends on the difference after this subtraction. Otherwise, the number of e-mails sent is a random number. It replies to all e-mail items not contained in the "Sent Items," "Outbox," or "Drafts" folders with a copy of itself as an attachment. If the infected user's version of Windows Scripting Host is greater than 5, it delays operation for a certain amount of time. Otherwise, it modifies another set of registry entries. It then drops a text file in the temporary directory and opens this file using C:\WINDOWS\Notepad.exe. Upon execution, it deletes the file.

VBS.Sargo.A@mm.int (Aliases: VBS.Nasara.A@mm, VBS/NastySarah@m) (Visual Basic Script Worm): VBS.Sargo.A@mm.int is an intended virus, coded to use MAPI. NOTE: The virus suffix ".int" indicates a threat that is intended to spread, but does not, due to bugs or errors in the viral code. The intention of this virus was to do the following: If MAPI is not installed, it attempts to spread by using Collaboration Data Objects for NT Server (CDONTS) of Microsoft SMTP Service, which is installed with IIS 4 or later. If it cannot find either, the worm then uses Microsoft Outlook. If the worm cannot find any of these programs, it displays following message and quits:

Hey! Haven't you heard! There's a VBS worm spreading by this very filename! You're lucky you didn't get hit! Forward this warning on to all of your contacts, so they won't get hit by the bug!

If the worm does find one of these programs, it deletes any e-mail message that includes the word "NASTYSARAH" in the subject or message. It then spreads by automatically replying to messages that you received previously, as follows:

Message: Hey! Thanks for your mail! I've been kind of busy lately, and haven't really had time to do a full reply, so, until I do, check this out.
Regards,
<User Name>
Attachment: NastySarah.jpg.vbs

If the recipient replies to that message, the virus then sends following message back to them. On May 31, the virus modifies the Autoexec.bat file to delete the entire contents of drive C.

W32/Matcher-B (W32 Worm): This is a variant of the W32/Matcher Win32 e-mail-aware worm. The worm arrives in an e-mail with the following characteristics:

Subject: Matcher
Body text: Want to find your love mates!!! Try this its cool... Looks and Attitude Matching to opposite sex.
Attached file: matcher.exe

If the attached file is launched it copies itself into the Windows System and temp directories, changing the system registry entry HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ to point to the infected file in the System directory. The worm will start to continuously send itself out using addresses from the Outlook address book. The worm also makes changes to the existing AUTOEXEC.BAT file on the C: drive, appending the following lines:

@echo off
echo from: Bugger
pause

W32.Update.Worm (Aliases: I-Worm.Mustard, W32.Mustard) (W32 Worm): This is a mass-mailing worm that can spread using Microsoft Outlook. The worm is written in a high-level language. However, for the e-mail spreading, the worm creates and executes a VBS script. This worm also can also spread using mIRC. This worm may also attempt to disable Norton AntiVirus, depending on which version is being used and under which operating system.

W32/Weather (Aliases: VBS/Weather, mIRC/Weather, Repah) (Win32 Worm): This is an e-mail-aware worm which incorporates a Visual Basic Script and mIRC component. When executed the worm drops files called c:\mirc\script.ini, d:\mirc\script.ini and c:\mail.vbs onto your local drives. It then copies itself as weather.txt.exe to the Windows and root directories. By using a filename with a double-extension some users may be fooled into thinking it is an innocent ASCII text file rather than a malicious executable program. Finally the worm runs the dropped c:\mail.vbs script which sends the worm as an e-mail attachment called weather.txt.exe to addresses found in the Outlook address book. The worm sends e-mails with the following characteristics:

Subject: Weather report
Body text: Hello. Yes, the weather's getting better, it's real sunny in some countries. Check the attached weather report for your country.
Attached file: weather.txt.vbs

The worm also sends the autoexec.bat file of the infected computer to an e-mail address based in the UK belonging to Rhape79, a member of the Ultimate Chaos virus writing gang.

W97M.Quest.A (Word 97 Macro Virus): If an infected document is opened in Microsoft Word 2000, then one of the following messages will be displayed:

He he he!! You have a insane mind!!
Look behind you! There is a monkey with three heads!
Hello I'm WM2K.Question and now I speak to you
Hello I'm WM2K.Question and I'm Very Crazy!
Do you believe to be intelligent?
Stop Pirates!!

If the date is May 10, 15, 20, or 25, the following message is displayed: “Who are You? Answer in this inputbox”. If you enter the answer "Nobody" the virus displays the message: “Well, you are lucky!! Bye.” If you enter anything else, the virus displays the message:” I'm sorry for you. You have entered a wrong Answer” and then it displays the following error message two times: “Error writing on drive C on INT 24.” However, the error is false, and the virus does not do anything malicious.

W97M.Thus.CV (Word 97 Macro Virus): When an infected document is opened, the virus checks active documents and the Normal.doc template for the comment line "NIST_32a" to determine whether the document or template is already infected. This is done to avoid multiple infections. If the comment line is not present, the document or template is then infected. After infection, the virus changes the Macro Protection setting of some Microsoft Office programs to Off. The following programs are affected:

Word 98/2000
Excel 98/2000
PowerPoint 98/2000

The virus then attempts to encrypt randomly chosen .exe and .vdb files that are greater than 12 bytes in size. If the encryption is successful, the file cannot be repaired.

WM97/Bleck-B (Word 97 Macro Virus): This is a variant of the WM97/Bleck-A Word macro virus. On August 31 this virus attempts to insert the following text at the beginning of the Word document:

"A CURSE FROM BLACKROSE TO SOMEONE HE HATES. HIJADIPUTA KANG HAYUP KA! BURAY MO, SAKA BURAY NI INA MO! HAYUP KA! SAYANG KA, HAYUP KA! HAYUP KA TALAGA! VIRGOBLACKROSE Virus Development Libmanan Camarines Sur"

WM97/Marker-HJ (Word 97 Macro Virus): Whenever a document is closed, the virus takes the information in File|Properties|Summary and attempts to ftp it to the Codebreakers site. It also attaches the sent information to the bottom of the macro as comments.

WM97/Marker-HL (Word 97 Macro Virus): WM97/Marker-HL is a Word macro virus which infects Microsoft Word documents. The virus creates a non-viral file called C:\version.dat, which it uses during replication.

WM97/Thus-EN (Word 97 Macro Virus): WM97/Thus-EN is a Word macro virus. On January 20th, this virus will use the Microsoft Office Assistant to display a message with the heading "PEPO PUNDA" and the text "hallo this little VIRUS is a little harmless.”

Trojans

Trojan Horse programs have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2001-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are descriptions of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that their anti-virus software detects. *At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
Backdoor.Acropolis	N/A	CyberNotes-2001-04
Backdoor.Netbus.444051	N/A	CyberNotes-2001-04
Backdoor.NTHack	N/A	CyberNotes-2001-06
Backdoor.Quimera	N/A	CyberNotes-2001-06
Backdoor.SMBRelay	N/A	CyberNotes-2001-10
Backdoor.WLF	N/A	CyberNotes-2001-08
Backdoor-JZ	N/A	CyberNotes-2001-02
BAT.Black		**Current Issue**
BAT.Install.Trojan	N/A	CyberNotes-2001-04
BAT.Trojan.DeltreeY	N/A	CyberNotes-2001-07
BAT.Trojan.Tally	N/A	CyberNotes-2001-07
BAT_DELWIN.D	N/A	CyberNotes-2001-05
BAT_EXITWIN.A	N/A	CyberNotes-2001-01
BioNet	3.13	CyberNotes-2001-07
BSE Trojan	N/A	CyberNotes-2001-07
DLer20.PWSTEAL	N/A	CyberNotes-2001-05
Eurosol	N/A	CyberNotes-2001-10
Fatal Connections	2.0	CyberNotes-2001-09
Flor	N/A	CyberNotes-2001-02
Freddy	beta 3	CyberNotes-2001-09
Gift	1.6.13	CyberNotes-2001-09
HardLock.618	N/A	CyberNotes-2001-04
Jammer Killah	1.2	CyberNotes-2001-10
JS.StartPage	N/A	CyberNotes-2001-07
Noob	4.0	CyberNotes-2001-09
PERL/WSFT-Exploit		**Current Issue**
PHP/Sysbat	N/A	CyberNotes-2001-02
PIF_LYS	N/A	CyberNotes-2001-02
PWSteal.Coced240b.Tro	N/A	CyberNotes-2001-04
SadCase.Trojan:	N/A	CyberNotes-2001-09
Scarab	1.2c	CyberNotes-2001-10
Troj/Futs	N/A	CyberNotes-2001-07
Troj/Keylog-C	N/A	CyberNotes-2001-08
Troj/KillCMOS-E	N/A	CyberNotes-2001-01
Troj/Unite-C	N/A	CyberNotes-2001-09
TROJ_AOL_EPEX	N/A	CyberNotes-2001-01
TROJ_AOLWAR.B	N/A	CyberNotes-2001-01
TROJ_AOLWAR.C	N/A	CyberNotes-2001-01
TROJ_APS.216576	N/A	CyberNotes-2001-03
TROJ_ASIT	N/A	CyberNotes-2001-07
TROJ_AZPR	N/A	CyberNotes-2001-01
TROJ_BADTRANS.A	N/A	CyberNotes-2001-08
TROJ_BAT2EXEC	N/A	CyberNotes-2001-01
TROJ_BCKDOR.G2.A		**Current Issue**
TROJ_BKDOOR.GQ	N/A	CyberNotes-2001-01
TROJ_BUSTERS	N/A	CyberNotes-2001-04
TROJ_CAINABEL151	1.51	CyberNotes-2001-06
TROJ_DARKFTP	N/A	CyberNotes-2001-03
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-05
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-04
TROJ_EUTH.152	N/A	CyberNotes-2001-08
TROJ_FIX.36864	N/A	CyberNotes-2001-03
TROJ_FUNNYFILE.A	N/A	CyberNotes-2001-09
TROJ_GLACE.A	N/A	CyberNotes-2001-01
TROJ_GNUTELMAN.A	N/A	CyberNotes-2001-05
TROJ_GOBLIN.A	N/A	CyberNotes-2001-03

Trojan	Version	CyberNotes Issue #
TROJ_GTMINESXF.A	N/A	CyberNotes-2001-02
TROJ_HAVOCORE.A	N/A	CyberNotes-2001-09
TROJ_HERMES	N/A	CyberNotes-2001-03
TROJ_HFN	N/A	CyberNotes-2001-03
TROJ_ICQCRASH	N/A	CyberNotes-2001-02
TROJ_IDENTD.B		**Current Issue**
TROJ_IE_XPLOIT.A	N/A	CyberNotes-2001-08
TROJ_IF	N/A	CyberNotes-2001-05
TROJ_INCOMM16A.S	N/A	CyberNotes-2001-09
TROJ_JOINER.15	N/A	CyberNotes-2001-02
TROJ_JOINER.I	N/A	CyberNotes-2001-08
TROJ_LASTWORD.A	N/A	CyberNotes-2001-09
TROJ_MATCHER.A	N/A	CyberNotes-2001-08
TROJ_MOONPIE	N/A	CyberNotes-2001-04
TROJ_MOONPIE.A		**Current Issue**
TROJ_MTX.A.DLL	N/A	CyberNotes-2001-09
TROJ_MYBABYPIC.A	N/A	CyberNotes-2001-05
TROJ_NAKEDWIFE	N/A	CyberNotes-2001-05
TROJ_NARCISSUS.A	N/A	CyberNotes-2001-09
TROJ_NAVIDAD.E	N/A	CyberNotes-2001-01
TROJ_PARODY	N/A	CyberNotes-2001-05
TROJ_PICSHOW.A	N/A	CyberNotes-2001-10
TROJ_PORTSCAN	N/A	CyberNotes-2001-03
TROJ_Q2001	N/A	CyberNotes-2001-06
TROJ_QZAP.1026	N/A	CyberNotes-2001-01
TROJ_RUNNER.B	N/A	CyberNotes-2001-03
TROJ_RUX.30	N/A	CyberNotes-2001-03
TROJ_SCOUT.A	N/A	CyberNotes-2001-08
TROJ_SUB7.21.E	2.1	CyberNotes-2001-05
TROJ_SUB7.22.D	.22	CyberNotes-2001-06
TROJ_SUB7.401315	N/A	CyberNotes-2001-01
TROJ_SUB7.MUIE	N/A	CyberNotes-2001-01
TROJ_SUB7.V20	2.0	CyberNotes-2001-02
TROJ_SUB722	2.2	CyberNotes-2001-06
TROJ_SUB722_SIN	N/A	CyberNotes-2001-06
TROJ_SUB7DRPR.B	N/A	CyberNotes-2001-01
TROJ_SUB7DRPR.C	N/A	CyberNotes-2001-03
TROJ_TPS	N/A	CyberNotes-2001-05
TROJ_TWEAK	N/A	CyberNotes-2001-02
TROJ_VBSWG_2B	N/A	CyberNotes-2001-07
TROJ_WEBCRACK	N/A	CyberNotes-2001-02
TROJ_WINMITE.10	N/A	CyberNotes-2001-08
Trojan.MircAbuser	N/A	CyberNotes-2001-04
Trojan.PSW.M2.14	N/A	CyberNotes-2001-07
Trojan.RASDialer	N/A	CyberNotes-2001-06
Trojan.Sheehy	N/A	CyberNotes-2001-05
Trojan.Taliban	N/A	CyberNotes-2001-07
Trojan.W32.FireKill	N/A	CyberNotes-2001-07
Trojan/PokeVB5	N/A	CyberNotes-2001-07
VBS.Cute.A	N/A	CyberNotes-2001-05
VBS.Delete.Trojan	N/A	CyberNotes-2001-04
VBS.Lumorg	N/A	CyberNotes-2001-09
VBS.Over.Trojan	N/A	CyberNotes-2001-10
VBS.SystemColor.A		**Current Issue**
VBS.Trojan.Noob	N/A	CyberNotes-2001-04
VBS.Zeichen.A	N/A	CyberNotes-2001-08
VBS_HAPTIME.A	N/A	CyberNotes-2001-09
VBS_IESTART.A		**Current Issue**

Trojan	Version	CyberNotes Issue #
W32.BatmanTroj	N/A	CyberNotes-2001-04
W32.BrainProtect	N/A	CyberNotes-2001-07
Y3K Rat	**1.6**	**Current Issue**

BAT.Black: This is a batch file Trojan that appends itself to the C:\Autoexec.bat file and attaches itself to the C:\Windows\Win.ini file. The file name of the batch file is BlackDay.bat. Due to bugs in the virus code, some parts are not executed.

PERL/WSFT-Exploit: This remote access Trojan is used by the SunOS/BoxPoison.worm to deface unpatched Microsoft IIS Webs Servers by overwriting the index/default page in the WWWROOT folder with the following text:

f@#! USA Government
f@#! PoizonBOx
(Substitute text has been used here for demonstration purposes)

This tool is used by an attacker to exploit the "Web Server Folder Traversal" Vulnerability. This vulnerability could allow an attacker to read, write, delete, or execute files on a remote system. They could also upload other programs to that system and execute them remotely.

TROJ_BCKDOR.G2.A (Aliases: BCKDOR.G2.A, BackDoor, Sub7): This is the server side of a hacking tool and enables a remote user running the client side of the tool to access an infected computer. The Trojan copies itself to the infected system and modifies the registry so that it is executed at every boot up. Upon execution, this Trojan copies itself to the infected system and creates a file with a random filename in the Windows directory. The Trojan then modified WIN.INI to execute its copy upon every Windows startup. It also modified the following registry to invoke the file it dropped when an executable file is executed:

HKEY_LOCAL_MACHINE\Software\Classes\exefile\shell\open\command to "second random dropped file "%1" %*"
HKEY_CLASSES_ROOT\exefile\shell\open\command to second random dropped file "%1" %*"

It then compromises network security by using Transfer Control Protocol (TCP) port 60606 to give system privileges to a remote user running the client side of this Trojan.

TROJ_IDENTD.B (Alias: IDENTD.B): This server side of a client-server Trojan allows a remote hacker access to an infected system. It compromises network security. Upon execution, this Trojan listens to port 113 and waits for a connection from the client side. Thereafter, a remote user running the client side of this Trojan may access the infected system.

TROJ_MOONPIE.A (Aliases: MOONPIE.A, Moon Pie 1.3 server): This server component of a memory-resident backdoor Trojan steals cached passwords and establishes an FTP server where remote users log in and gain access to an infected computer. This program is coded and compiled in Borland Delphi. Its Circulating program is compressed with UPX. Upon execution, this server program copies itself to two files, ASDFLKHJ.DFG in the root directory of the infected Drive C:\ and SYSIDIT.EXE in the Windows system directory. It creates the following Autostart registry entry to execute SYSIDIT.EXE in subsequent reboots:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\Run\Regedit="%winsysdir%\sysidit.exe"

It reinstates the modified key whenever the infected user attempts to disable the autostart registry with Regedit. It registers itself as a service process that is not seen in the Task List. It opens and listens to TCP ports 27160, 25686, and 25982. Port 25686 is for the FTP server it establishes. The remaining ports are used for client and server communications.

The client program for this Trojan has the following capabilities:

Get system information and cached passwords
Change Windows colors as well as some desktop settings
File manager – upload, download, and execute file
Registry manager

Disable/enable CTRL-ALT-DEL
Hide/show Window's Start button and System Tray
Open/close CD-Rom
Displays message
Ping
FTP server

VBS_IESTART.A (Aliases: IESTART.A, IESTART, VBS/IESTART.GEN): This Visual Basic Script (VBS) Trojan file drops an .HTA file that modifies the default page of Internet Explorer. It has no destructive payload.

VBS.SystemColor.A: This is a Trojan horse that is written in Visual Basic Script. Once it is executed, it copies itself to C:\Windows\Filemon.exe. It then starts to repeatedly copy Explorer.exe as C:\Windows\System\Systemcolor\Color. As a result, the computer may run out of space on the hard disk and stop responding. You may not be able to run Windows. It also adds the value Filemon to the registry key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run so that it runs when Windows starts.

Y3K Rat: This is a revamped version of an old Trojan, now capable of ruining computer hard drives, breaking through many firewalls and transmitting cached passwords and copies of all activity on an infected computer to the attacker by e-mail. The server can be pre-configured with many options. One is to deny local connections (you trying to connect to the server with the client on your computer). Another is to disallow the edit server to read the settings again after they are saved. Another option is to configure an ICQ UIN to be notified when your computer comes online. The edit server also can configure the registry infection. So, manual removal might be slightly different depending on whether the "hacker" changed anything. This version has a Napster spy feature, which allows the "hacker" to see what you are doing on Napster.